DETAILED ACTION

1. This office correspondence is response to the applicant's after response filed on 01/21/2009.

EXAMINER'S AMENDMENT

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Applicant's representative, **John J. Torrente** (Reg. No. 26,359), and examiner arranged a telephone interview on April 07, 2009 and the interview agenda was to reach an agreement of allowance of claims with examiner amendment would make to these claims as follows:

In the claims:

Claims have been rewritten as follows:

Claim 1 (Currently amended): A digital signature generating apparatus that generates a digital signature of digital data, comprising:

a receiving unit that receives one of a first command and a second command, the first command including information indicating one of a plurality of secret keys, the plurality of secret keys being included in the digital signature generating apparatus, the second command including a hash value of the digital data;

a secret key changing unit that changes a secret key used by the digital signature generating apparatus to a secret key specified by the first command, if the first command is received by the receiving unit; and

a digital signature generating unit that generates the digital signature of the digital data from ~~a~~ the hash value extracted from the second command, if the second command is received by the receiving unit,

wherein the digital signature generating unit encrypts the hash value extracted from the second command using the secret key specified by the first command, in order to generate the digital signature of the digital data.

Claim 2 (Previously presented): The digital signature generating apparatus according to claim 1, wherein the digital signature generating apparatus is an IC card.

Claim 3 (Previously presented): The digital signature generating apparatus according to claim 1, wherein the digital signature generating apparatus is an apparatus including a multi-application operating system.

Claims 4-13 (Cancelled).

Claim 14 (Previously presented): The digital signature generating apparatus according to claim 1, further comprising:

a storage unit that stores the plurality of secret keys.

Claim 15 (Previously presented): The digital signature generating apparatus according to claim 1, wherein the digital data includes image data.

Claims 16-19 (Canceled).

Claims 20-28 (Cancelled).

Claim 29 (Currently Amended) A method for controlling a digital signature generating apparatus that generates a digital signature of digital data, the method comprising:

a receiving step of receiving one of a first command and a second command, the first command including information indicating one of a plurality of secret keys, the plurality of secret keys being included in the digital signature generating apparatus, the second command including a hash value of the digital data;

a secret key changing step of changing a secret key used by the digital signature generating apparatus to a secret key specified by the first command, if the first command is received in the receiving step; and

a digital signature generating step of generating the digital signature of the digital data from ~~a~~ the hash value extracted from the second command, if the second command is received in the receiving step,

wherein the hash value extracted from the second command is encrypted in the digital signal generating step using the secret key specified by the first command, in order to generate the digital signature of the digital data.

Claim 30 (Previously Presented) The method according to claim 29, wherein the digital signature generating apparatus is an IC card.

Claim 31 (Previously Presented) The method according to claim 29, wherein the digital signature generating apparatus is an apparatus including a multi-application operating system.

Claim 32 (Previously Presented) The method according to claim 29, wherein the digital signature generating apparatus includes a storage unit that stores the plurality of secret keys.

Claim 33 (Previously Presented) The method according to claim 29, wherein the digital data includes image data.

Allowable Subject Matter

2. Claims 1-3, 14-15, 29-33 are allowed. The following is an examiner's statement of reasons for allowance: In interpreting the claims, in light of the Specification and the examiner's amendments has been made to the claims, the Examiner finds the claimed invention to be patentably distinct from the prior art of record.

3. Hirata et al (Foreign patent application JP2002300150) is concerned a receiving unit that receives one of a first and second command, the first command including information indicating one of a plurality of secret keys, the plurality of secret keys being

included in the digital signature generating apparatus, a digital signature generating unit that generates the digital signature of the digital data if the second command is received by the receiving unit.

4. Kawakita et al (Foreign patent application JP10031626) is concerned disclosing that a secret key changing unit that changes a secret key used by the digital signature generating apparatus to a secret key specified by the first command, if the first command is received by the receiving unit.

5. However the totality of each element and/or step in claims 1-3, 14-15, 29-33 are not alluded to in the combined art of Hirata and Kawakita. Their teachings either individually or in combination failed to teach or suggest the method recited in claim 1. More specifically, the combination of Hirata and Kawakita does not teach or suggest "the digital signature generating unit encrypts the hash value extracted from the second command using the secret key specified by the first command, in order to generate the digital signature of the digital data" as recited in claim 1. Similarly, the combination of Hirata and Kawakita does not teach or suggest "the digital signature generating unit that generates the digital signature of the digital data from the hash value extracted form the second command" as recited in claim 1. Accordingly, claim 1, and 29 is allowable over the combination of Hirata and Kawakita. So, Claims 1-3, 14-15, 29-33 are allowable by virtue of their dependency upon claim 1, and 29 and also due to additional limitations recited in these claims. Therefore, for the foregoing reasons, examiner withdraws of the rejection of claims 1-3, 14-15, 29-33 under 35 USC §103(a) as being obvious over Hirata in view of Kawakita.

7. However, the prior art of record fails to teach or suggest some of the steps of the present claim invention. Examiner performed an updated search and unable to find any prior art to disclose all the steps mentioned in the independent claims.

8. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

9. Claims 1-3, 14-15, 29-33 are patentable.

10. Claims 4-13, and 16-28 are cancelled.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mohammad w. Reza whose telephone number is 571-272-6590. The examiner can normally be reached on M-F (9:00-5:00).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, MOAZZAMI NASSER G can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Nasser G Moazzami/ /Mohammad W Reza/

Supervisory Patent Examiner, Art Unit 2436 Examiner, Art Unit 2436